v3.3 Release Notes for Forcepoint Behavioral Analytics

Release Notes | Forcepoint Behavioral Analytics | v3.3 | 20-Dec-2019

Use the Release Notes to find information about what's new and improved in Forcepoint Behavioral Analytics version 3.3.

Features

Certified DDP Compatibility

As part of the Human Point System, Forcepoint Behavioral Analytics version 3.3 is certified to deliver Dynamic Data Protection (DDP) with the following combinations of Forcepoint DLP:

Forcepoint Behavioral Analytics	Forcepoint DLP	Forcepoint One Endpoint
3.3	8.7.0	19

DDP requires the use of the Forcepoint One Endpoint as the Endpoint Security solution. The Mac OS X version of the Forcepoint One Endpoint is not compatible for the DDP solution.

Sizing recommendations

Forcepoint Behavioral Analytics supports up to 100,000 concurrent monitored entities with risk score production for use in the Analytics Dashboard, the Entity Timeline, and for Dynamic Data Protection.

Entity source priority is configurable

When consuming an Entity, whether or not it is monitored is determined by the priority of the entity's source. The priority of a given source is set within the configuration. (RPP-13428)

Open Source Framework has been moved

The Open Source Framework button and report have been removed from the About modal that users can access under the Settings drop-down. The Forcepoint Behavioral Analytics Open Source Framework list is now a file that lives outside the application, here. (RPP-13466)

New EULA Subscription Agreement needs to be accepted

The EULA Subscription Agreement has been updated for the latest release of the product. Every user, including existing users, will need to accept the EULA before using the application. (RPP-13310)

New boolean field “has_incident” added

We have added a new boolean field on Forcepoint DLP events called "has_incident". This field can be used to query for events that do or do not have an associated incident. (RPP-13332)

Behaviors page Results table tool-tip

An information tool-tip has been added to the Behaviors page Results table to inform users that the results are returned at random and if they would like to get different results to click Apply again. (RPP-13487)

Entity Timeline and Dashboard are no longer automatically computed

The disable_timeline_compute configuration has been removed from the Master Data Service(MDS) application configuration. With the removal of this configuration, the Entity Timeline will no longer automatically compute upon navigating to the Entity Timeline page. Entity Timeline computations will now be managed by a daily compute intervals cron job that will run along side the hourly compute dashboard job.

There is a configured jenkins job that runs every hour at ten minutes past to compute the dashboard and timeline to ensure consistent results. Given there is no need for computations to be running until Monitored Entities exist in the application, the job is disabled by default. Toggling it on allows for those compute jobs to run via Jenkins.

Additionally, out of the box, the risk_level/publish endpoint in the ueba-publisher-service will no longer trigger a compute dashboard job in MDS. (RPP-13437, RPP-13524)

Note

The cron job added here computes scores based on "now" and will produce incorrect results if your data is not streaming in "real time". If your data is, for instance, streaming deferred 2 hours, you should disable this job and run your own.

Note

This job will compute updated scores once an hour. You will still need to compute a full dashboard once upfront to use the analytic dashboard.

Clear Analytics cache updated

The "clear analytics cache" endpoint should only succeed if there are no active or pending compute intervals jobs. MDS endpoints that delete analytic cache entries will now respond with a "503 Service Unavailable"error if there are any ongoing jobs. Outdated cache entries are no longer cleared from the Analytics Cache when modifying Analytics Configuration (models/scenarios/etc). (RPP-13504, RPP-13395)

Entity Profile page updated for unresolved Entities

The Entity Profile page has been updated to no longer display the Risk level tab, the Entity Timeline tab, the Identifiers table, and the add attributes and add entity features buttons for an unresolved entity. Additionally, given the entity is unresolved on the entity profile page, only their raw alias will be displayed. (RPP-13306)

Disk Destination entity role

The Forcepoint DLP event/incident connector in the Public API now populates the "Disk Destination" entity role on Forcepoint Behavioral Analytics events when converting Forcepoint DLP events that include a destination disk. (RPP-13340)

Apply button disabled after clicking

On the Behaviors page, the Apply button is now disabled after it is clicked until configuration changes are made, a new scenario is loaded, or the request completes. This helps ensure MDS does not become overburdened with ad hoc interval computation requests. (RPP-13401)

Rabbit requeues messages with redelivery flag

If the system fails unexpectedly during the processing of messages consumed from rabbit, rabbit will requeue these messages with a redelivery flag set to “true”. Any message that has the redelivery flag set to “true” will immediately be sent to the error queue without any further processing. However, if the system fails unexpectedly due to a bad event, some threads may be in the middle of processing valid events. These valid events will be subject to this same "redelivery" behavior and will go to the error queue along with the bad event once systems are brought back online. If users wish to see these valid events in their system, the valid events will need to be manually re-ingested. Additionally, if one were to investigate message payloads in the rabbitmq UI and requeue messages from this UI, these requeued events would also have their redelivery flag set to true and the system would route them to the error queue. (RPP-13398)

Limiting entity computations on the Behavior page

If the app config property behaviors_use_cache(default value is true) is set to false, then cache results were computed on the fly for the Behaviors page, which with a large enough set of monitored entities can become quite costly. Now, when the above mentioned property is set to false, the number of entities computations are run for on the Behaviors page is limited by using the value defined in behaviors_compute_entity_limit (default value is 10,000) (RPP-13505)

Cache refreshing reduced

Excessive cache refreshing has been cut down to only the essentials needed for correctly calculating scores. This improves performance by not needing to wait for ElasticSearch to refresh the cache when the operation is not needed. (RPP-13195)

Export entity risk level

The Kafka topic ENTITY_RISK_LEVEL has been deprecated but retained. The Kafka new topic EXPORT_ENTITY_RISK_LEVEL has been added.

Format:

```
{
        "entity_id": "John Smith",
        "timestamp": "2019-12-31T23:59:59.999Z",
        "risk_level": 5,
        "aliases": [{
                "alias": "johnsmith@badcompany.com",
                "type": "email"
        }, {
                "alias": "john_smith",
                "type": "username"
```

```
            }]
    }
```

Aliases-to-export are configurable via UEBA Publisher Service configuration: export_alias_types. This configuration takes a list of string alias types to include in EXPORT_ENTITY_RISK_LEVEL. (RPP-13055)

Delayed email message processing is no longer supported

Delayed processing of email messages to guarantee email threading/quoting for nightly batch jobs containing out-of-order emails is no longer supported. As a result quoted text detection will only detect quoted regions of text if the email with the original attestation of the text is processed by ingest before the later email with the quoted text. (RPP-13393)

Unresolved entities updated

Unidentified entities that were discovered during event ingest have stopped persisting. Any requests made by the UI for an unresolved entity will result in a "default" entity in which the actor id, display name, and alias will all be the same value. These entities will still have an entity detail view where their events can be viewed, however no attributes or features are able to be added to them. (RPP-13304)

Compute dashboard job on ROSE and on a configurable schedule

As part of its regularly running compute dashboard job, ueba-publisher-service would also remove risk level and risk level override attributes that fell outside of a configurable retention window. This functionality has now been moved to ROSE and runs on a configurable schedule. The default schedule is to run daily at 00:05 and to keep 30 days worth of risk level and risk level override attributes. Additionally, an API endpoint is provided at v1/attribute/truncate_risk_levels where a user can manually trigger a truncation job to execute. (RPP-13445)

New Entity Source field

Any given entity can now include an `entity_source` field. This allows us to delimit whether or not a given entity can be promoted to the primary entity based on entity source prioritization. (RPP-13423)

All analytics cache writes must be done through compute intervals job

All analytics cache writes occur through compute intervals jobs. This means that the Entity Timeline and Behaviors Page no longer compute missing intervals ad hoc. If scenario results are not available for the given query criteria the Entity Timeline page

displays an error message. The Behavior page will return partial results that are already computed and are stored in the cache, but such results could be incomplete. If there are no results available for the given query criteria, the page displays an error message. (RPP-13465)

New endpoint for Event summary export

A new endpoint in the Public API has been created to allow the export of event summary data, like that found in the UI on the Explore Page. The endpoint path is: `event_export/summary` and returns the count of events broken down by mode for the time ranges of "all time" and "last 24 hours". (RPP-13426)

New endpoint for Top Entities

A new endpoint has been created in the Public API to retrieve the current data that exists in the analytic cache and is displayed in the UI on the Analytic Dashboard page under Top Entities. The new endpoint is 'analytics_export/entity' and accepts a size parameter for the number of entities you want returned, with a default value of 100. The endpoint returns the top X entities by total risk score and includes the individual scores for each model for each interval. (RPP-13454)

Configurable Node server timeouts

Node server timeouts are now configurable. The new ansible variable is:

```
{{ro_ui_server_timeout_seconds}},
```

This variable defaults to 120 seconds and controls the server timeout for both nginx and the UI's API.

Modify the following:

```
{{/usr/share/ro-ansible/roles/ro-ui/defaults/main.yml}}
```

Then change the new variable:

```
{{ro_ui_server_timeout_seconds}}
```

After changing this, use the following Jenkins job to deploy the change.

```
{{deploy-ueba-ui}}
```

(RPP-12149)

Known Issues

A list of resolved and known issues in this release is available to Forcepoint Behavioral Analytics customers here.

If you are not currently logged in to the Forcepoint support website, clicking the link brings up a My Account login prompt. Log in to view the list.